KELLEY DRYE & WARREN LLP
A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400
3050 K STREET, NW
WASHINGTON, D.C. 20007-5108

(202) 342-8400

FACSIMILE
(202) 342-8451
www.kelleydrye.com

NEW YORK, NY
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES
MUMBAI, INDIA

DIRECT LINE: (202) 342-8640
EMAIL: dcrock@kelleydrye.com

February 23, 2009

VIA ECFS

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Annual Customer Proprietary Network Information Compliance Certification; EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e), Affinity Networks, Inc. hereby provides its Annual Customer Proprietary Network Information Compliance Certification. Please feel free to contact me if you have any questions regarding this filing.

Sincerely,

Devin L. Crock

DC01/CROCDE/369556.2

Annual Customer Proprietary Network Information Certification
Pursuant to 47 C.F.R. § 64.2009(e)
EB Docket No. 06-36
February 2009

Name of Company: Affinity Network, Inc.
Form 499 Filer ID: 809136
Name of Signatory: Raymond A. Perea
Title of Signatory: General Counsel

I, Raymond A. Perea, certify that I am an officer of Affinity Network, Inc. ("ANI"), and acting on behalf of ANI, that I have personal knowledge that ANI has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how ANI's procedures ensure the company is in compliance with the requirements set forth in sections 64.2001 *et seq.* of the Commission's rules.

ANI has not taken any actions (instituted proceedings or filed petitions at either state commissions, courts, or at the FCC) against data brokers in the past year. ANI has no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available (*e.g.,* through news media), regarding the processes pretexters are using to attempt to access CPNI. The steps the company has taken to protect CPNI include updating its CPNI practices and procedures and conducting new training designed to ensure compliance with the FCC's modified CPNI rules.

ANI has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Raymond A. Perea
General Counsel
Affinity Network, Inc.

Date: 2.17.09

Attachment A

Customer Proprietary Network Information Certification

Affinity Network, Inc. ("ANI") has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC" or "Commission") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 – 64.2011 of the Commission's rules. This attachment summarizes those practices and procedures.

Safeguarding against pretexting

- ANI takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI based on customer-initiated contacts. ANI is committed to notify the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against pretexters and data brokers.

Training and discipline

- ANI trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out ANI's obligation to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, (d) obtain customers' informed consent as required with respect to its use for marketing purposes, and (e) keep records regarding receipt of such consent, customer complaints regarding CPNI and the use of CPNI for marketing campaigns.

- ANI employees are required to review ANI's CPNI practices and procedures set forth in ANI's CPNI policy and related training material and to acknowledge their comprehension thereof.

- ANI has an express disciplinary process in place for violation of the company's CPNI practices and procedures. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

ANI's use of CPNI

- ANI may use CPNI for the following purposes:

    - to initiate, render, maintain, repair, bill and collect for services;
    - to protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
    - to provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
    - to market additional services to customers that are within the same categories of service to which the customer already subscribes;
    - to market services formerly known as adjunct-to-basic services; and
    - to market additional services to customers *with the receipt of informed consent via the use of opt-in or out-out, as applicable.*

- ANI does not disclose or permit access to CPNI to track customers that call competing service providers.

- ANI discloses and permits access to CPNI where required by law (*e.g.*, under a lawfully issued subpoena).

Customer approval and informed consent

- ANI has implemented a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This system also allows for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.

  - Prior to any solicitation for customer approval, ANI notifies customers of their right to restrict the use of, disclosure of, and access to their CPNI.
  - ANI uses opt-in approval when using or disclosing CPNI for purposes other than permitted under opt-out approval or in 47 USC 222 and the FCC's CPNI rules.
  - A customer's approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval.
  - Records of approvals are maintained for at least one year.
  - ANI provides individual notice to customers when soliciting approval to use, disclose, or permit access to CPNI.
  - The content of ANI's CPNI notices complies with FCC rule 64.2008(c).

  Opt-out

  - ANI uses opt-out for the marketing of communications related services by its employees outside the category of service to which the customer subscribes and for affiliate marketing of any communications related services. When ANI uses opt-out approval, ANI provides notification by electronic or written methods and waits at least 30 days after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. ANI provides customers with opt-out notifications every two years. When using e-mail for opt-out notices, ANI complies with the additional requirements set forth in FCC rule 64.2008(d)(3). Additionally, ANI makes available to every customer an opt-out method, at no additional charge, that is available 24 hours a day, seven days a week.

  Opt-in

  - ANI uses opt-in approval for marketing by independent contractors and joint venture partners and for then marketing of non-communications related services by itself and its affiliates. When ANI uses opt-in approval, ANI provides notification consistent with FCC rule 64.2008(c).

  One time use

  - After authentication, ANI uses oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice comports with FCC rule 64.2008(f).

Additional safeguards

- ANI maintains for at least one year records of all marketing campaigns that use its customers' CPNI, including a description of each campaign and the CPNI used, the products offered as part of the campaign, and instances where CPNI was disclosed to third parties or where third parties were allowed access to CPNI. Such campaigns are subject to a supervisory approval and compliance review process, the records of which also are maintained for a minimum of one year.

- ANI has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules for outbound marketing situations and maintenance of records.

- ANI designates one or more officers, as an agent or agents of the company, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in FCC rule 64.2009(e).

- ANI will provide written notice to the Commission in accordance with the requirements of FCC rule 64.2009(f) if ever its opt-out mechanisms malfunction in the manner described therein.

- For customer-initiated telephone inquiries regarding or requiring access to CPNI, ANI authenticates the customer (or its authorized representative), through a pre-established password, without prompting through the use of readily available biographical or account information. If the customer cannot provide a password, then ANI only discloses call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record.

- For online customer access to CPNI, ANI authenticates the customer (or its authorized representative) without the use of readily available biographical or account information. After the customer has been authenticated, ANI utilizes a customer-established password to authorize account access. ANI establishes passwords and has employed back-up authentication for lost or forgotten passwords consistent with the requirements of FCC rule 64.2010(e).

- ANI discloses CPNI to customers at ANI's retail locations if the customer first presents a valid photo ID matching the customer's account information.

- ANI notifies customers immediately of any account changes, including address of record, authentication, online account and password related changes.

- ANI may negotiate alternative authentication procedures for services that ANI provides to business customers that have both a dedicated account representative and a contract that specifically addresses ANI's protection of CPNI.

- In the event of a breach of CPNI, ANI will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs ANI to delay notification, or ANI and the investigatory party agree to an earlier notification. ANI will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.